Exercise 6

Foundation of Cryptography, Fall 2011

Itay Berman

January 9, 2012

4.a Denote the view as $(r, in, \overline{a}_{1,\ldots,t})$ where r is the random coins of D, in is D's input and $\overline{a}_{1,\ldots,t} \in (\{0,1\}^n)^t$ are the first t oracle answers D received. Note that since both D^{B} and D^{Π} views includes r and in, then it is suffice to prove that $\Pr[\mathsf{B}(\overline{q}_{1,\ldots,t}) = \overline{a}_{1,\ldots,t}] = \Pr[\Pi(\overline{q}_{1,\ldots,t}) = \overline{a}_{1,\ldots,t}]$, for every $t \in \mathbb{N}$, where $\overline{q}_{1,\ldots,t}$ are the first t queries of D. We prove this using induction on t: the base case is clear. Assuming for $t-1$ we will show that $\Pr[\mathsf{B}(q_t) = a_t \mid \mathsf{B}(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] = \Pr[\Pi(q_t) = a_t \mid \Pi(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}]$. Consider two cases:

Case 1: $\exists i \in [t-1]\colon q_t = q_i$. In this case, from the definition of B we get

$$\Pr[\mathsf{B}(q_t) = a_t \mid \mathsf{B}(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] = \begin{cases} 1 & a_t = a_i \\ 0 & Otherwise \end{cases},$$

and from the definition of Π we get

$$\Pr[\Pi(q_t) = a_t \mid \Pi(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] = \begin{cases} 1 & a_t = a_i \\ 0 & Otherwise \end{cases}.$$

Hence, $\Pr[\mathsf{B}(q_t) = a_t \mid \mathsf{B}(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] = \Pr[\Pi(q_t) = a_t \mid \Pi(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}]$.

Case 2: $\forall i \in [t-1]\colon q_t \neq q_i$. In this case the conditioning above are irrelevant and thus

$$\begin{aligned}\Pr[\mathsf{B}(q_t) = a_t \mid \mathsf{B}(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] &= \Pr[\mathsf{B}(q_t) = a_t] \\ &= 2^{-n} \\ &= \Pr[\Pi(q_t) = a_t] \\ &= \Pr[\mathsf{B}(q_t) = a_t \mid \Pi(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}].\end{aligned}$$

The induction assumption yields that

$$\begin{aligned}\Pr[\mathsf{B}(\overline{q}_{1,\ldots,t}) = \overline{a}_{1,\ldots,t}] &= \Pr[\mathsf{B}(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] \cdot \Pr[\mathsf{B}(q_t) = a_t \mid \mathsf{B}(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] \\ &= \Pr[\Pi(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] \cdot \Pr[\Pi(q_t) = a_t \mid \Pi(\overline{q}_{1,\ldots,t-1}) = \overline{a}_{1,\ldots,t-1}] \\ &= \Pr[\Pi(\overline{q}_{1,\ldots,t}) = \overline{a}_{1,\ldots,t}],\end{aligned}$$

as required.

4.b: Assume towards a contradiction that $\mathcal{F} \oplus \mathcal{G}$ if not PRF, namely $\exists$ PPT A, and $p \in \text{poly}$ such that

$$\left|\Delta^{\mathsf{A}}_{\mathcal{F}_n \oplus \mathcal{G}_n, \Pi_n}\right| = \left|\Pr_{h \leftarrow \mathcal{F}_n \oplus \mathcal{G}_n}[\mathsf{A}^h(1^n)] - \Pr_{\pi \leftarrow \Pi}[\mathsf{A}^\pi(1^n)]\right| \geq \frac{1}{p(n)},$$

for infinitely many n's. Now, consider the following algorithms:

Algorithm 1 ($\mathsf{B}_{\mathcal{F}}$)**.**

Input: 1^n.

Oracle: *Function* $\phi \colon \{0,1\}^n \mapsto \{0,1\}^n$.

1. *Sample* $g \leftarrow \mathcal{G}_n$.
2. *Construct* $o = \phi \oplus g$.
3. *Emulate* $\mathsf{A}^o(1^n)$.

Algorithm 2 ($\mathsf{B}_{\mathcal{G}}$)**.**

Input: 1^n.

Oracle: *Function* $\phi \colon \{0,1\}^n \mapsto \{0,1\}^n$.

1. *Sample* $f \leftarrow \mathcal{F}_n$.
2. *Construct* $o = f \oplus \phi$.
3. *Emulate* $\mathsf{A}^o(1^n)$.

Note that since A is PPT and $\mathcal{F}$,$\mathcal{G}$ are efficient ensembles, then $\mathsf{B}_{\mathcal{F}}, \mathsf{B}_{\mathcal{G}}$ are PPT . Considering $\mathsf{B}_{\mathcal{F}}$, if $\phi \leftarrow \mathcal{F}_n$ then $o \leftarrow \mathcal{F}_n \oplus \mathcal{G}_n$ and if $\phi \leftarrow \Pi_n$ then $o \leftarrow \Pi_n$ (as xoring with random value gives a random value). Thus,

$$\left|\Delta^{\mathsf{B}_{\mathcal{F}}}_{\mathcal{F}_n, \Pi_n}\right| = \left|\Delta^{\mathsf{A}}_{\mathcal{F}_n \oplus \mathcal{G}_n, \Pi_n}\right| \geq \frac{1}{p(n)}$$

for infinitely many n's. Considering $\mathsf{B}_{\mathcal{G}}$, if $\phi \leftarrow \mathcal{G}_n$ then $o \leftarrow \mathcal{F}_n \oplus \mathcal{G}_n$ and if $\phi \leftarrow \Pi_n$ then $o \leftarrow \Pi_n$. Thus,

$$\left|\Delta^{\mathsf{B}_{\mathcal{G}}}_{\mathcal{G}_n, \Pi_n}\right| = \left|\Delta^{\mathsf{A}}_{\mathcal{F}_n \oplus \mathcal{G}_n, \Pi_n}\right| \geq \frac{1}{p(n)}$$

for infinitely many n's.

If $\mathcal{F}$ is PRF then follows $\mathsf{B}_{\mathcal{F}}$ we get a contradiction. If $\mathcal{G}$ is PRF then follows $\mathsf{B}_{\mathcal{G}}$ we get a contradiction. At any case we get a contradiction, thus $\mathcal{F} \oplus \mathcal{G}$ is PRF.